

CASE NO.: AM9-98-028-US2
Serial No.: 09/575,740
May 13, 2004
Page 2

PATENT
Filed: May 22, 2000

1. (previously presented) A method for complicating a coincidence attack in a system for protecting content on recordable media, comprising:

providing a single media key;

transforming the media key using a position-specific function with each of a sequence of positions to render a sequence of position-dependent media keys; and

encrypting each position-dependent media key with a respective position-dependent device key.

2. (previously presented) A system for complicating a coincidence attack in a system for protecting content on recordable media, comprising:

a media key block (MKB), the MKB including plural encrypted entries, each entry having a position in the MKB, each entry being established at least in part by transforming a key number using a position number representing the position in the MKB of the respective key number.

3. (original) The system of Claim 2, wherein an entry is established by a media key.

4. (original) The system of Claim 2, wherein each entry is established by the same media key as all other entries, the media key being combined with each of a sequence of positions to render a sequence of position-dependent media keys.

1053-100.AM2

CASE NO.: AM9-98-028-US2
Serial No.: 09/575,740
May 13, 2004
Page 3

PATENT
Filed: May 22, 2000

5. (original) The system of Claim 4, wherein each position-dependent media key is encrypted by a respective device key.

6. (original) The system of Claim 5, further comprising plural players, each having a device key of known position with which to decrypt the media key to play content encrypted with the media key.

7-9 (canceled).

10. (original) A computer program device, comprising:
- a computer program storage device including a program of instructions usable by a decryption computer, comprising:
 - logic means for receiving a media key block (MKB) having plural positions, each position having a number related thereto;
 - logic means for accessing a device key, the device key being associated with a position corresponding to one of the positions of the MKB, the position associated with the device key being known to the decryption computer;
 - logic means for decrypting the number at a position in the MKB corresponding to the position associated with the device key to render a decrypted position-dependent media key; and
 - logic means for reverse transforming the position-dependent media key with a number representing the position of the position-dependent media key in the MKB, to render a media key.

1003-100.AM2

CASE NO.: AM9-98-028-US2
Serial No.: 09/575,740
May 13, 2004
Page 4

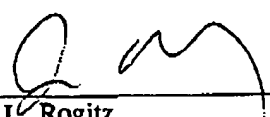
PATENT
Filed: May 22, 2000

11. (original) The computer program device of Claim 10, further comprising logic means for decrypting content using the media key.

1053-100.AM2

CASE NO.: AM9-98-028-US2
Serial N .: 09/575,740
May 13, 2004
Page 5

PATENT
Filed: May 22, 2000



John L. Rogitz
Registration No. 33,549
Attorney of Record
750 B Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JLR:jg

1053-100.AM2